(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
11 avril 2002 (11.04.2002)

PCT

(10) Numéro de publication internationale
WO 02/29742 A1

(51) Classification internationale des brevets[7] : G07F 19/00, 7/10

(21) Numéro de la demande internationale : PCT/FR01/03072

(22) Date de dépôt international : 5 octobre 2001 (05.10.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0012706 5 octobre 2000 (05.10.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SOCIETE NTSys SA** [FR/FR]; Centre Scientifique A. Mairaux, 64, Chemin des Mouilles, F- 69130 Ecully (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **MONTIEL, Jacky** [FR/FR]; Résidence Charrière Blanche, Frênes 1, F-69130 Ecully (FR).

(74) Représentant commun : **SOCIETE NTSys**; Centre Scientifique A. Mairaux, 64, Chemin des Mouilles, F- 69130 Ecully (FR).

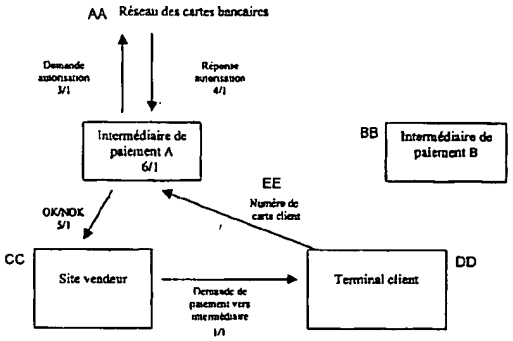
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien

[Suite sur la page suivante]

(54) Title: SECURE INTERNET PAYING AGENT WITH MOBILE TELEPHONE VALIDATION

(54) Titre : MANDATAIRE DE PAIEMENT SECURISE INTERNET AVEC VALIDATION PAR TELEPHONE MOBILE



AA...BANK CARD NETWORK
3/1...AUTHORISATION REQUEST
4/1...AUTHORISATION REPLY
6/1...PAYMENT INTERMEDIARY A
BB...PAYMENT INTERMEDIARY B
CC...SELLER SITE
1/1...PAYMENT REQUEST TO INTERMEDIARY
DD...CLIENT TERMINAL
EE...CLIENT NUMBER

(57) **Abstract:** The invention concerns an Internet server acting as secure paying agent, that is relaying all payment requests to bank card payment systems requiring card number input. The client is registered once on the server by supplying among others his bank card number and by installing a standard X509 certificate on his terminal, protected by a security code known only to him. When purchasing from his initialised PC, the payment request is relayed to the agent server which authenticates the client through his X509 certificate, causing the security code to be requested on the client terminal. The client using such a secure system, accepts not to challenge a purchase carried out by the agent. A request made from an anonymous PC (that is non-initialised), is blocked until a secure validation procedure is carried out. Three validating procedures are proposed: 1) validation from a WAP mobile telephone; 2) validation from a normal mobile telephone; 3) validation for a WAP mobile telephone with WIM module.

[Suite sur la page suivante]

WO 02/29742 A1

(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Serveur Internet agissant comme mandataire de paiement sécurisé, c'est à dire relayant des requêtes de paiement vers des systèmes de paiement par carte bancaire demandant la saisie du numéro de carte. Le client s'enregistre une fois sur le serveur en fournissant entre autres son numéro de carte bancaire et en installant un certificat X509 standard sur son terminal, protégé par un code sécurité connu de lui seul. Lors d'un achat depuis son PC initialisé, la requête de paiement est relayée vers le serveur mandataire qui authentifie le client à travers son certificat X509, provoquant la demande du code de sécurité sur le terminal client. Le client utilisant un tel systéme sécurisé, accepte de ne pas contester d'achat passé par le mandataire. Une requête d'achat passée depuis un PC anonyme (c'est à dire non initialisé) au mandataire, est bloquée sur le mandataire jusqu'à ce q'une procedure de validation sécurisée soit effectuée. Trois procédures de validation sont proposées: 1. validation depuis du téléphone mobiel WAP 2. validation depuis un téléphone mobile normal 3. validation depuis du téléphone mobile WAP avec module WIM.

MANDATAIRE DE PAIEMENT SECURISE INTERNET AVEC VALIDATION PAR TELEPHONE MOBILE

Problématique ciblée et Etat de l'art

Une des problématiques du paiement sur Internet est de réduire les contestations de transactions passées en ligne, en mettant en place des solutions garantissant la sécurité et la non répudiation par le client.

Par ailleurs, les solutions sécurisées existantes sont essentiellement basées sur un accès par terminal PC. Le développement du marché des mobiles, crée de nouveaux besoins d'achat en ligne multi-terminaux et disposer d'un système cohérent unique permettant de payer des achats en boutique depuis son PC, depuis un PC anonyme, ou depuis son téléphone mobile serait un avantage certain.

Les solutions proposées aujourd'hui en termes de paiement en ligne depuis les PC avec navigateur utilisent l'un des moyens suivants :

1. introduction d'un terminal sécurisé auxiliaire disposant d'un lecteur de carte bancaire (système du type de celui proposé par la société CyberCOMM),
2. utilisation de certificats électroniques, comme SET
3. transmission du numéro de carte en ligne sur une liaison chiffrée (ex : en utilisant un protocole comme SSL exploitant de la cryptographie publique du type Diffie-Helmann)

La première approche nécessite la mise en place d'un terminal spécifique (écran, clavier, processeur) chez le client utilisant la carte bancaire à puce comme les terminaux d'achat classiques. Ce moyen est considéré comme non répudiable.

La deuxième approche est basée sur des certificats non standards et n'est pas strictement non répudiable car basé sur du logiciel installé sur des postes très ouverts comme les PC des clients.

La troisième approche est la plus utilisée aujourd'hui car ne nécessitant aucune installation de la part du client, mais c'est elle qui déclenche le plus de fraudes parce que le numéro de carte est transmis sans authentification du client. Le fait de disposer d'un numéro de carte bancaire (information semi-confidentielle) suffit pour passer des ordres au nom d'une personne. Un générateur de numéro cohérents de cartes bancaires peut être utilisé à cet effet.

Les solutions de paiement sécurisé par carte bancaire sur Internet s'appuyant sur la troisième approche, mettent en œuvre aujourd'hui des intermédiaires de paiement sécurisé par carte (notés IPSC). Un IPSC assure l'interface entre l'Internet et un réseau de cartes bancaire.

La communication entre le client et l'intermédiaire bancaire utilise un des principes suivants :

- le numéro de carte est transmis par le client à chaque échange (figure 1)
- le numéro de carte est stocké sur le terminal client et c'est un logiciel qui se charge de réaliser la transaction avec le serveur intermédiaire bancaire du vendeur
- le client est enregistré auprès de l'IPSC, qui conserve son numéro de carte et qui interroge le réseau cartes bancaires à chaque transaction.

Pour ce qui est du paiement par les mobiles les solutions proposées restent limitées à la gestion du système d'information de l'opérateur de mobile.

Définitions

On entend par faiblement non répudiable, un dispositif transactionnel qui en utilisation normale utilise des informations connues du seul client pour signer la transaction et ne pouvant être transmises vers un hôte extérieur que si le client réalise une opération non autorisée, pouvant créer un trou de sécurité comme la mise en place d'un espion dans son système de signature électronique.

Un système faiblement non répudiable, si le client s'engage à ne pas opérer certaines opérations et en accepte les règles contractuellement, devient non répudiable par le client.

Objectif du dispositif

L'objectif principal du dispositif est d'apporter une amélioration aux solutions de type transmission du numéro de carte systématique, permettant de limiter les risques de fraude à une fraction négligeable des transactions en introduisant la qualité de "non répudiation faible". Le deuxième objectif est de permettre des transactions unifiées Web/téléphone mobile.

Description du dispositif

Le dispositif proposé utilise un serveur Internet (8/2) agissant comme mandataire de paiement orienté client et intervenant en intermédiaire dans les échanges entre des systèmes IPSC (6/2) et le terminal client (7/2). Le serveur mandataire peut également effectuer des demandes d'autorisation vers des systèmes de paiement autres. Ce dispositif utilise un mécanisme de signature faiblement non répudiable pour authentifier les requêtes de paiement en provenance des clients. Son originalité est qu'il s'appuie sur des accès multi-terminaux. On distinguera 4 types de terminaux :

- le PC fixe (étant supposé à domicile)
- le PC occasionnel, dit PC anonyme (ex : borne multimédia publique)
- le téléphone mobile simple
- le téléphone mobile de type WAP, avec ou sans module WIM.

Lorsque la prise de commande est faite sur un terminal anonyme, le serveur mandataire de paiement requiert une validation par un terminal téléphone mobile.

Dans l'utilisation de base, c'est-à-dire depuis un PC fixe personnel, le client installe un certificat standard délivré par le mandataire de paiement à l'inscription comprenant entre autres une clé privée à importer dans le navigateur du PC. Lors de l'importation, le client choisit :

- un code personnel appelé code de sécurité (CODE_S) qui protège l'usage de son certificat
- un code de validation (CODE_V) qui sera utilisé pour valider les transactions.

Le bouton achat d'un transaction en ligne comprend en paramètres signés par le site vendeur : le contenu de la transaction, le prix, le code vendeur et consiste en un lien vers une demande de paiement vers le serveur mandataire. L'action sur ce bouton déclenche une liaison SSL entre le poste client et le mandataire de paiement et le passage des paramètres précédents. Le passage en mode SSL provoque l'accès au certificat client et donc une demande d'entrée du code de sécurité pour son déverrouillage local. Si le code est correct la liaison est établie et le serveur mandataire authentifie le client.

Le code vendeur passé en paramètre sert à établir le relais vers le bon IPSC (celui du vendeur) et à vérifier que cet IPSC accepte bien le mode de paiement du client. L'agent de sécurité dispose de plusieurs interfaces pour simuler les échanges d'un client avec les divers IPSC.

Lorsque le client intervient sur une borne anonyme ou chez un commerçant qui saisit en ligne la prise de commande pour son compte, celle-ci a été initialisée pour ne pas accéder au certificat. Dans ce cas les paramètres sont passés simplement en clair vers le serveur mandataire qui bloque le relayage en attente de validation par téléphone mobile et en affichant sur le poste client un numéro de transaction fixé par lui.

Pour chaque achat à valider, ce numéro unique identifie la transaction (vendeur, commande, client) et doit être signé par le serveur mandataire.

Trois cas de validation sont traités :

1. Cas du téléphone simple (figure 3)
2. Cas du téléphone WAP simple (figure 4)
3. Cas du téléphone WAP avec module WIM : authentification forte du client (figure 5)

Note :

Le téléphone mobile peut être à la fois considéré comme un terminal de prise de commande et de déclenchement de paiement. La prise de commande se fait comme sur un terminal de type PC.

Fonctionnement détaillé

Inscription /Installation

L'inscription du client auprès du serveur mandataire (figure 2-b) est réalisée de manière strictement confidentielle : on peut utiliser un enregistrement en ligne avec SSL par exemple ou un enregistrement au guichet.

Une procédure de validation par les exploitants du serveur mandataire, peut-être demandée. Elle doit assurer que les informations relevées à l'inscription sont valides.

Si le client a demandé un enregistrement pour PC fixe, le serveur mandataire produit un certificat électronique à base de clés publiques de type X509 émis avec sa clé privée au client par messagerie (10/2). Le certificat est encapsulé dans un format qui déclenche l'auto-installation sur le PC client. A l'installation du certificat, le client est invité à définir son code de protection des clés CODE_S, connu de lui seul et utilisé localement.

Si le client a demandé la validation par mobile, il fournit son numéro de mobile et choisit un autre code de sécurité, appelé code de validation CODE_V connu de lui seul et du serveur mandataire.

Les données fournies par le client et conservées sur le serveur mandataire sont :

- l'identité (nom, prénom)
- son numéro de carte
- l'adresse de livraison habituelle
- optionnellement : numéro de GSM
- le CODE_V.

Validation de l'identité client

Suivant la rigueur de la procédure souhaitée, il peut y avoir validation manuelle ou automatique, ou simplement aucune validation (acceptation de toutes les inscriptions) sauf des contrôles de non ré-inscription. En particulier des contrôles de réutilisation sur les messages électroniques et numéro de carte permettent de réduire les effets de ré-inscription.

Transactions

Depuis son PC initialisé

Les achats sont réalisés par un simple hyperlien vers le serveur mandataire par le protocole HTTP, les données de la transaction étant passées en paramètres. Ces données sont signées par le vendeur pour garantir l'intégrité vis-à-vis du vendeur.

La requête de paiement reçue au serveur mandataire permet d'authentifier le client de manière certaine, car la requête en mode SSL provient d'un PC fixe avec certificat. Dans ce cas, la requête est automatiquement validée et immédiatement relayée.

Depuis un PC anonyme

Si la requête est émise depuis un PC anonyme, le relayage est bloqué sur le serveur mandataire en attente de validation par le canal mobile (l'agent n'a pas authentifié de client). Le serveur mandataire demande l'identité du client et émet un numéro de transaction unique signé par lui pour la validation qui s'opère selon un des 3 modes autorisés.

Validation

1. Validation par téléphone

Le client appelle un numéro fixe, qui le met en communication avec un serveur vocal interactif ; il est invité à entrer le numéro unique de transaction, affiché sur l'écran de prise de commande; le serveur restitue par synthèse vocale le descriptif de la commande ; si celui-ci est correct, le client entre son code de validation CODE_V.

La passerelle envoie une requête de paiement chiffrée et signée par elle contenant : l'identificateur de transaction et le CODE_V introduit.

2. Validation WAP simple :

Dans ce cas le client établit une connexion WAP/ SSL vers le service validation du serveur mandataire de paiement ; le client s'identifie par son nom et prénom puis entre son code de validation CODE_V

3. Validation WAP avec module WIM ("WAP Identity Module")

Ce cas est identique sur le principe au cas 2, sauf que le terminal WAP dispose d'une capacité de signature électronique garantissant l'authentification du client ; dans ce cas, le CODE_V est signé par le module WIM avec les paramètres de la transaction.

Note :
Dans les cas 2 et 3 (validation WAP), la passerelle peut utiliser une méthode de mémorisation de l'identité client par Cookie. Le Cookie est un enregistrement en clair ASCII comprenant le nom, prénom du client signé par le serveur mandataire.

Exemple d'implémentation

Ce dispositif a été implémenté sur un serveur sous système Linux avec un pare-feu frontal sous Linux, et un IPSC opérationnel. Le système utilise HTTPS pour les échange SSL entre le PC client et l'agent de sécurité.

La validation par mobile a été réalisée par un terminal WAP, selon le mode d'accès simple. L'authentification depuis le téléphone mobile s'opère par nom prénom, puis introduction du code de sécurité passé en session SSL.

Revendications

1. Dispositif de mandatement pour les paiements sécurisés en ligne sur Internet sur des boutiques qui utilisent le chiffrement SSL pour la transmission du numéro de carte sans authentification du client vers un serveur d'autorisation bancaire, caractérisé en ce qu'il
   - comprend un moyen d'inscription des clients permettant de transmettre au mandataire le numéro de carte une seule fois à l'inscription, et ceci de manière sécurisée par liaison SSL
   - s'interpose au cours d'une transaction d'achat dans les échanges entre le terminal client et le serveur d'interrogation du réseau cartes bancaires de la boutique, d'une part en identifiant et authentifiant le client grâce à un mécanisme propre de signature électronique, et d'autre part en transmettant le numéro de carte client, mémorisé à l'inscription client, vers l'intermédiaire bancaire par la liaison SSL habituelle, sans authentification du mandataire de la part de l'intermédiaire bancaire.
2. Dispositif de mandatement de paiement selon les revendications 1, caractérisé par le fait qu'il utilise pour chaque client un certificat X509 standard généré sur le serveur mandataire à l'inscription client et transmis par messagerie avec la clé privée associée pour être importé dans le navigateur client, puis utilisé ensuite pour authentifier les clients dans les liaisons HTTP dans les transactions de paiement.
3. Dispositif de mandatement de paiement selon les revendications 1, caractérisé par le couplage possible à un dispositif auxiliaire permettant la validation par le téléphone mobile simple ou WAP, exploitant l'authentification du client par ce système auxiliaire et l'usage d'un code de validation connu seulement du client et du serveur mandataire.

Figure 1 : Etat de l'art

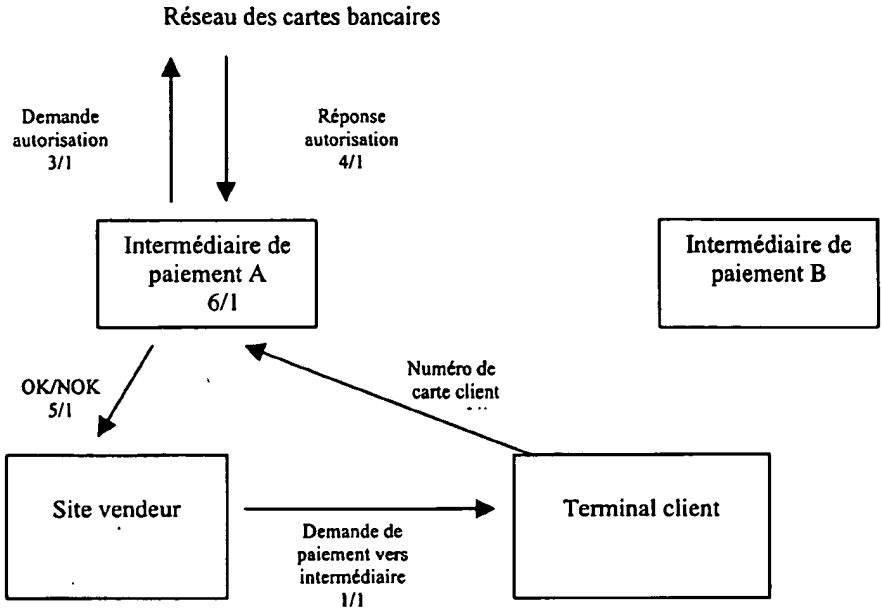


Figure 2-a : Transaction depuis PC initialisé

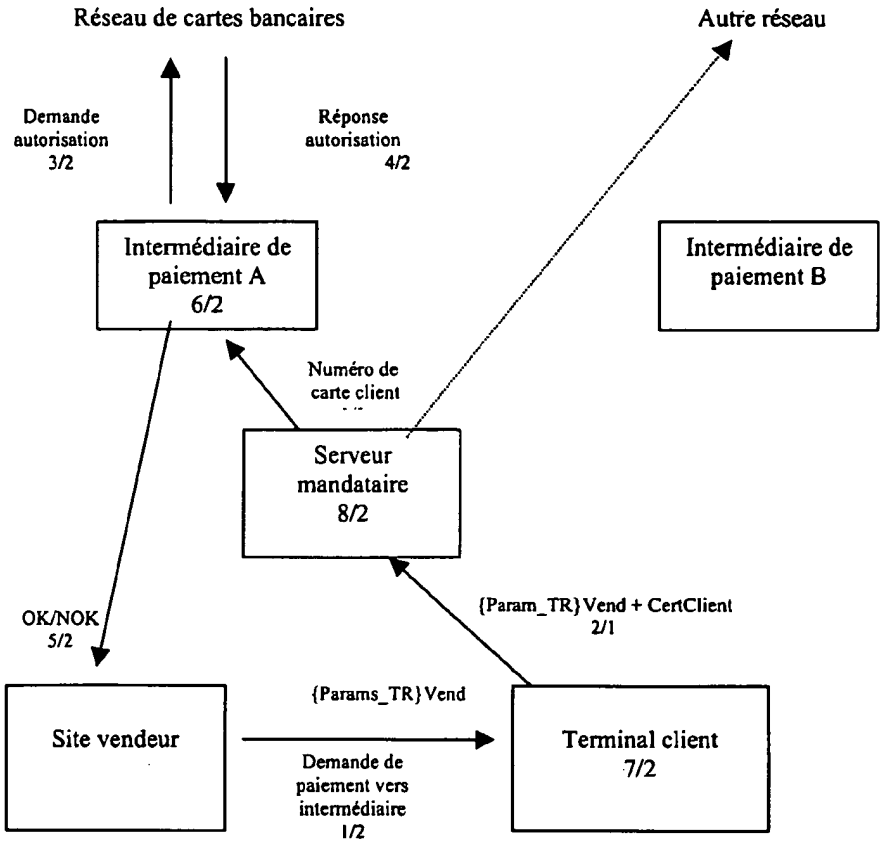


Figure 2-b: Inscription client sur PC initialisé

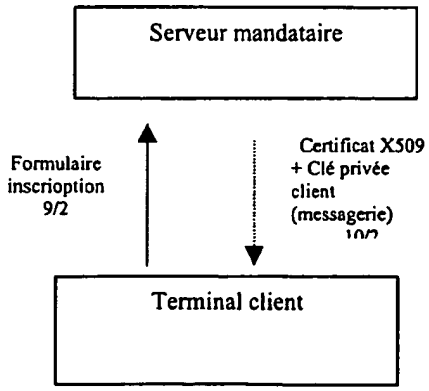


Figure 3 : Validation directe par GSM

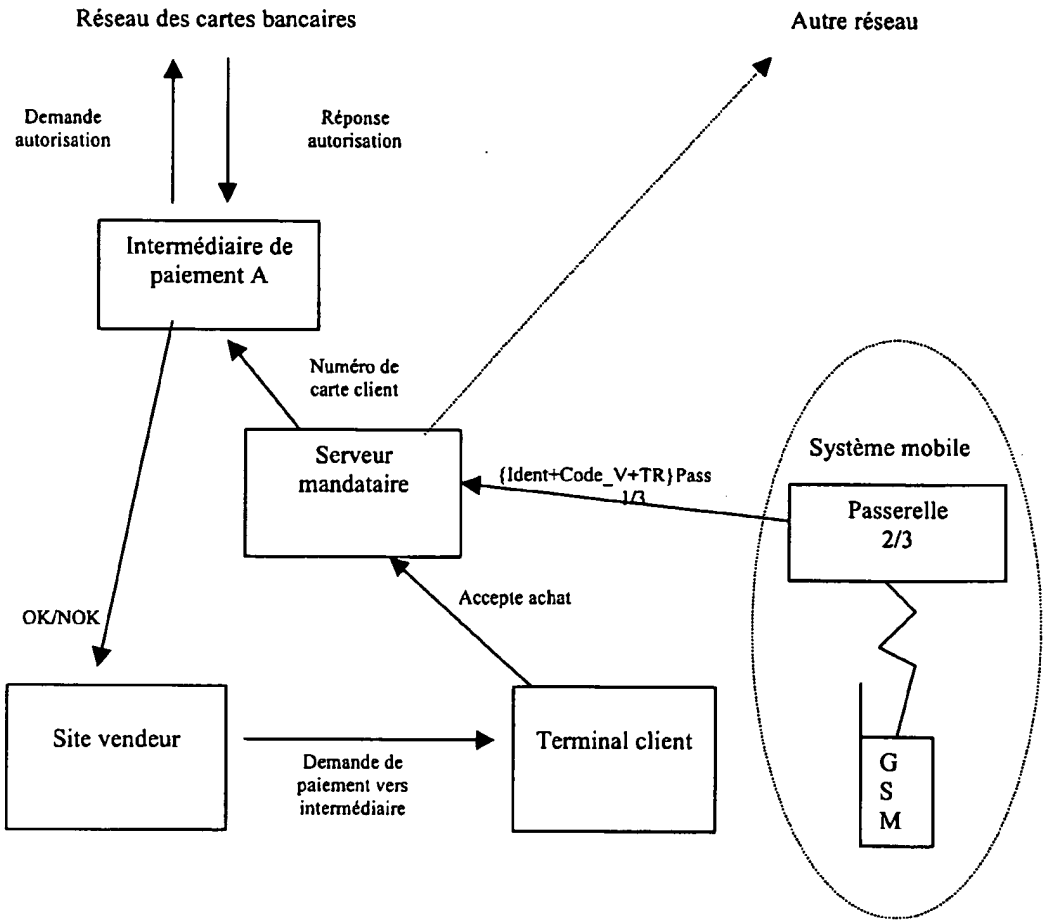


Figure 4 : Validation WAP simple

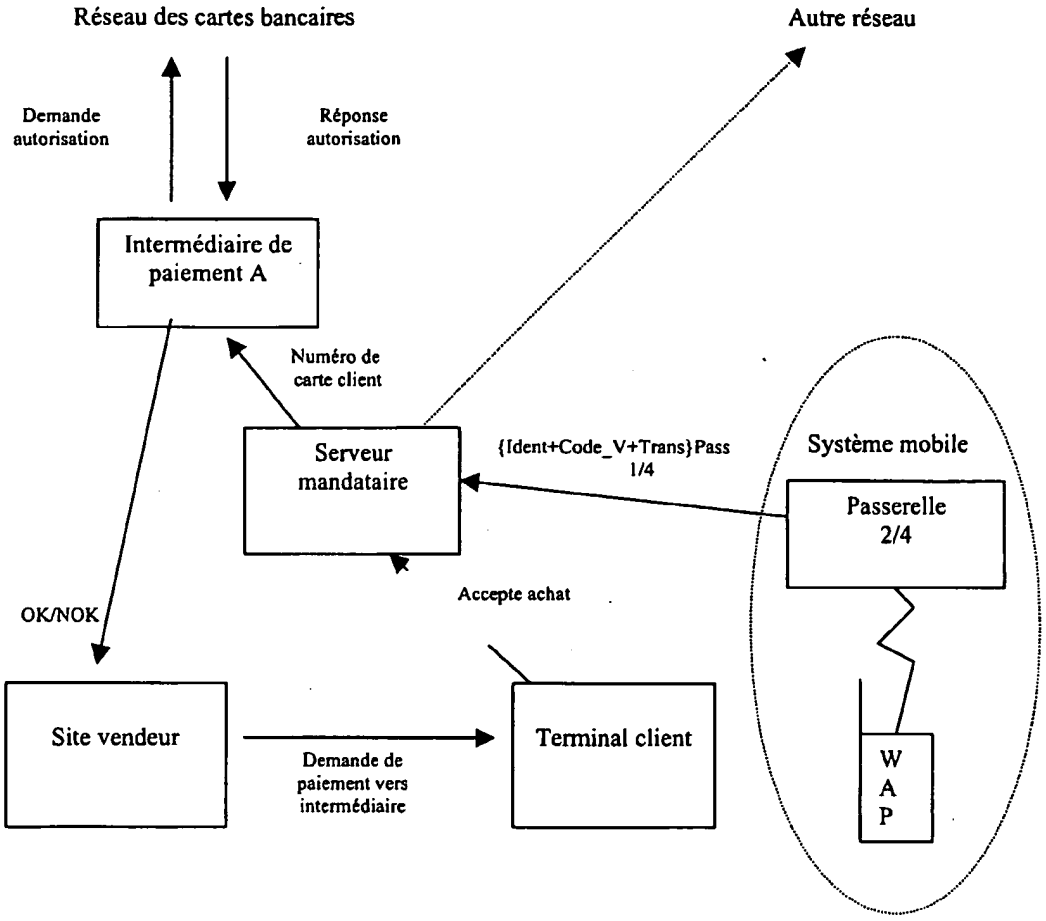
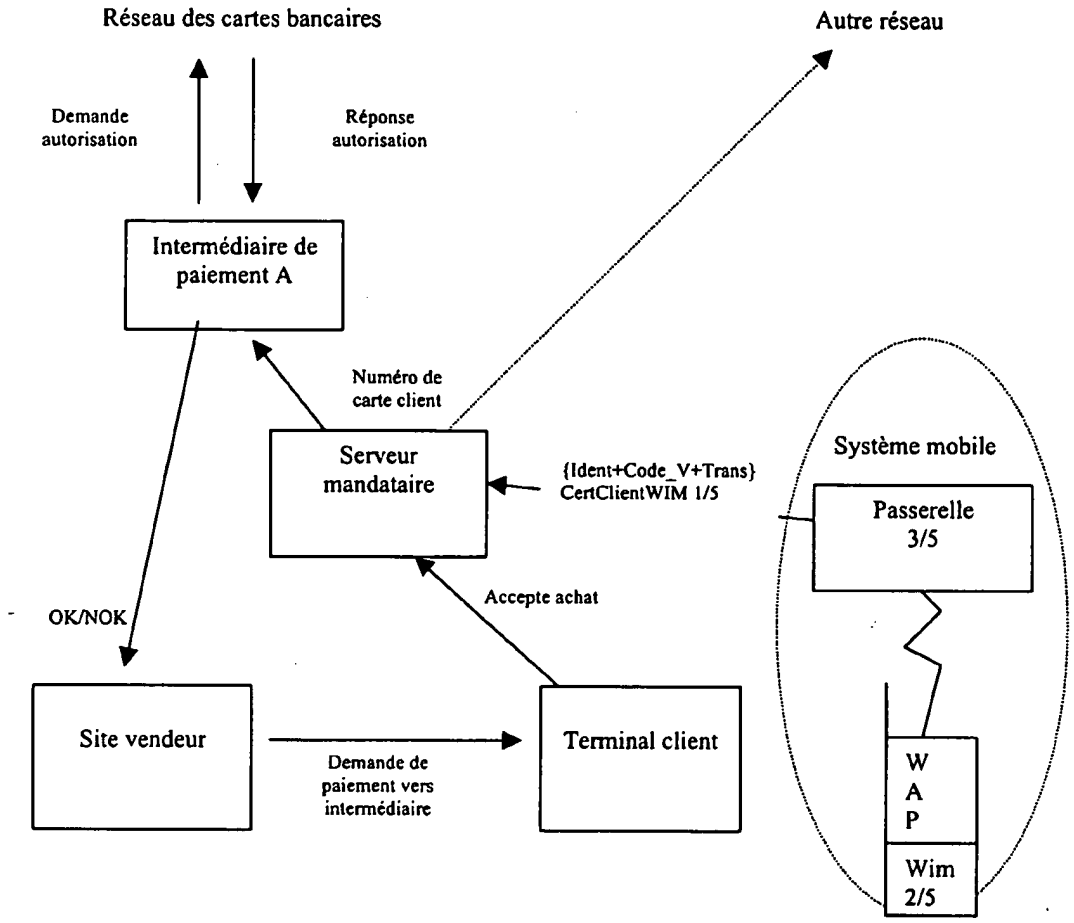


Figure 5 : Validation WAP avec module WIM



INTERNATIONAL SEARCH REPORT

Inte al Application No
PCT/FR 01/03072

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 026 166 A (LEBOURGEOIS JOHN H) 15 February 2000 (2000-02-15) column 5, line 14 -column 7, line 48 figures 1,3A-3B	1,2
A	WO 99 14711 A (ANDRASEV AKOS) 25 March 1999 (1999-03-25) page 10, line 24 -page 16, line 8 figures 1-3	1,3

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 February 2002	04/03/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Papastefanou, E

Form PCT/ISA/210 (second sheet) (July 199

INTERNATIONAL SEARCH REPORT

Int[illegible]onal Application No
PCT/FR 01/03072

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	VAN THANH D: "Security issues in mobile ecommerce" DATABASE & EXPERT SYSTEMS APPLICATIONS, DEXA,WIEN,AT, 4 September 2000 (2000-09-04), pages 412-425, XP002158270 page 415, paragraph 4 -page 417, paragraph 3 page 422, paragraph 1 -page 425, paragraph 1 figures 4,5 ---	1-3
A	EP 1 028 401 A (CITIBANK NA) 16 August 2000 (2000-08-16) paragraph '0008! - paragraph '0010! paragraph '0025! - paragraph '0034! figures 1,2 ---	1,2
A	US 6 014 650 A (ZAMPESE DAVID) 11 January 2000 (2000-01-11) figure 3 column 3, line 38 -column 5, line 39 -----	1

INTERNATIONAL SEARCH REPORT

Int nal Application No
PCT/FR 01/03072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6026166 A	15-02-2000	AU 1105599 A	10-05-1999
		EP 1033010 A1	06-09-2000
		JP 2001521329 T	06-11-2001
		WO 9921321 A1	29-04-1999
WO 9914711 A	25-03-1999	HU 9802109 A1	28-04-1999
		AU 9362498 A	05-04-1999
		EP 1021802 A2	26-07-2000
		WO 9914711 A2	25-03-1999
EP 1028401 A	16-08-2000	CN 1266240 A	13-09-2000
		EP 1028401 A2	16-08-2000
		JP 2000322486 A	24-11-2000
US 6014650 A	11-01-2000	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Den Internationale No
PCT/FR 01/03072

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F19/00 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 6 026 166 A (LEBOURGEOIS JOHN H) 15 février 2000 (2000-02-15) colonne 5, ligne 14 -colonne 7, ligne 48 figures 1,3A-3B ---	1,2
A	WO 99 14711 A (ANDRASEV AKOS) 25 mars 1999 (1999-03-25) page 10, ligne 24 -page 16, ligne 8 figures 1-3 --- -/--	1,3

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
25 février 2002	04/03/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Papastefanou, E

RAPPORT DE RECHERCHE INTERNATIONALE

De Internationale No
PCT/FR 01/03072

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	VAN THANH D: "Security issues in mobile ecommerce" DATABASE & EXPERT SYSTEMS APPLICATIONS, DEXA,WIEN,AT, 4 septembre 2000 (2000-09-04), pages 412-425, XP002158270 page 415, alinéa 4 -page 417, alinéa 3 page 422, alinéa 1 -page 425, alinéa 1 figures 4,5 ---	1-3
A	EP 1 028 401 A (CITIBANK NA) 16 août 2000 (2000-08-16) alinéa '0008! - alinéa '0010! alinéa '0025! - alinéa '0034! figures 1,2 ---	1,2
A	US 6 014 650 A (ZAMPESE DAVID) 11 janvier 2000 (2000-01-11) figure 3 colonne 3, ligne 38 -colonne 5, ligne 39 -----	1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 01/03072

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 6026166	A	15-02-2000	AU	1105599 A	10-05-1999
			EP	1033010 A1	06-09-2000
			JP	2001521329 T	06-11-2001
			WO	9921321 A1	29-04-1999
WO 9914711	A	25-03-1999	HU	9802109 A1	28-04-1999
			AU	9362498 A	05-04-1999
			EP	1021802 A2	26-07-2000
			WO	9914711 A2	25-03-1999
EP 1028401	A	16-08-2000	CN	1266240 A	13-09-2000
			EP	1028401 A2	16-08-2000
			JP	2000322486 A	24-11-2000
US 6014650	A	11-01-2000	AUCUN		